Smart inverters' vulnerability to cyberattacks needs to be identified and countered, according to researchers

November 29 2022, by Patrick Lejtenyi

Credit: mobius, CC BY-SA 3.0 , via Wikimedia Commons

The emergence of distributed energy resources (DERs)—facilities owned by individuals or small companies that can generate, store and return power to energy grids—is transforming the way power is used across the world.

The technology is becoming more prevalent as society looks for alternative sources of energy, but its rapid growth brings with it a new field of vulnerabilities open to cyberattacks.

DERs like home-based solar panels or electric vehicle chargers rely on field devices known as smart inverters to interface with power grids. As a new study by Concordia researchers shows, these devices' reliance on digital information and communication technology can be attacked in multiple ways by malicious actors, with serious repercussions for the public.

The paper, published in *IEEE: Transactions on Power Electronics*, surveys the landscape of smart inverter cybersecurity and identifies attack strategies at the device and grid level. It also looks at ways to defend against, mitigate and prevent them.

"We are still in the first decade of trying to understand the problem and identifying the most prominent risks," says the paper's co-author Jun Yan, associate professor at the Concordia Institute for Information Systems Engineering.

"Threats are inevitable. We have so many homeowners and third parties using these devices that having a perfect line of defense is impossible. We must look at our strategic priorities to start."

Yuanling Li, a Concordia Ph.D. student and research intern at Ericsson's

Global Artificial Intelligence Accelerator (GAIA), is the paper's lead author.

Risks at the device and grid levels

The researchers describe how attacks on smart inverters can take multiple forms, from threats to individual devices to the entire grid. Attacks on devices can disrupt communications between the device and the utility regulating energy flow or with other devices, but attacks on hardware are also possible.

They identify reconnaissance, replay, DDoS and Man-in-the-Middle as possible attack strategies on communications links between the inverters and devices. Tactics such as physical firmware attacks and hall spoofing, which involves the manipulation of electromagnetic fields around a device, target hardware.

At the microgrid level, the researchers note the possibility of cyberattacks on centralized control architectures and distributed control systems. Many of these attacks are designed to inject false data into the communications stream between the device and the regulator or block commands from the control to the devices.

These can lead to oscillations of power, voltage and frequency, and severely impede the microgrid's ability to distribute energy.

Part of a global network

The research was carried out as part of the Mitacs-Ericsson GAIA multi-institutional research initiative that links a network of researchers in Canada, the United States, India and Europe. As one of 25 Concordia graduate students participating in the initiative, Li has been researching

further into ethical hacking techniques to identify vulnerabilities in critical infrastructure.

"We use AI technologies in penetration testing of cyber-physical smart grids," he says. "The goal is to use deep reinforcement learning to find efficient and automatic ways to penetrate smart grids and create a negative physical impact."

As a leading member of the National Cybersecurity Consortium, Yan points out that Concordia is uniquely qualified to lead the fight against this emerging threat.

"This paper will provide us with a good starting point for our many research projects. For the broader research community, this lays out the solutions that exist and where are the gaps that still require one," he says.

"It can also help the industry review their practices and improve their baseline security."

More information: Li Yuanliang et al, Cybersecurity of Smart Inverters in the Smart Grid: A Survey, *IEEE Transactions on Power Electronics* (2022). DOI: 10.1109/TPEL.2022.3206239

Provided by Concordia University